SECURE SPACE NETWORKING

June 5, 2003

Howard Weiss
NASA/JPL/SPARTA
410-872-1515
hsw@sparta.com

AGENDA

- Background
- Space Security Issues, Threats, Requirements
- Security Paradigms
- Applicable Security Standards
- Summary

Hackers reportedly seize military satellite

Mon, 01 Mar 1999 17:00:33 GMT
Reuters

Latest News Index Similar story search

Hackers have seized control of one of Britain's military communication satellites and issued blackmail threats, The Sunday Business newspaper reported.

The newspaper, quoting security sources, said the intruders altered the course of one of Britain's four satellites that are used by defence planners and military forces around the world.

The sources said the satellite's course was changed just over two weeks ago. The hackers then issued a blackmail threat, demanding money to stop interfering with the satellite. "This is a nightmare scenario," said one intelligence source. Military strategists said that if Britain were to come under nuclear attack, an aggressor would first interfere with military communications systems.

"This is not just a case of computer nerds mucking about. This is very, very serious and the blackmail threat has made it even more serious," one security source said.

Police said they would not comment as the investigation was at too sensitive a stage. The Ministry of Defence made no comment.

Related stories:
Key services at risk from hackers
"E-Nazi" hacker attack spurs ISP to Linux upgrade
News Burst: Virtual country 'nuked' in cyberwar
Chinese hackers sentenced to death
Pentagon hackers banished from cyberspace
Hackers threaten Mexican government

Latest News Index Similar story search

HACKER NEWS NETWORK

1999 - http://www.hackernews.com

Security Analysis of Satellite Command and Control Uplinks

By Brian Oblivion, L0pht Heavy Industries

"Many critical information paths flow over satellites orbiting our earth. A box floating in space seems to be a likely target for hacker groups or renegade nation-states…

There are two methods of compromising a satellite by an external threat vector. One is an attack directly on the Satellite by a rogue Ground Station. The second is an attack on the Master Ground Station…

Space mission protocol design information is available on NASA sites..."

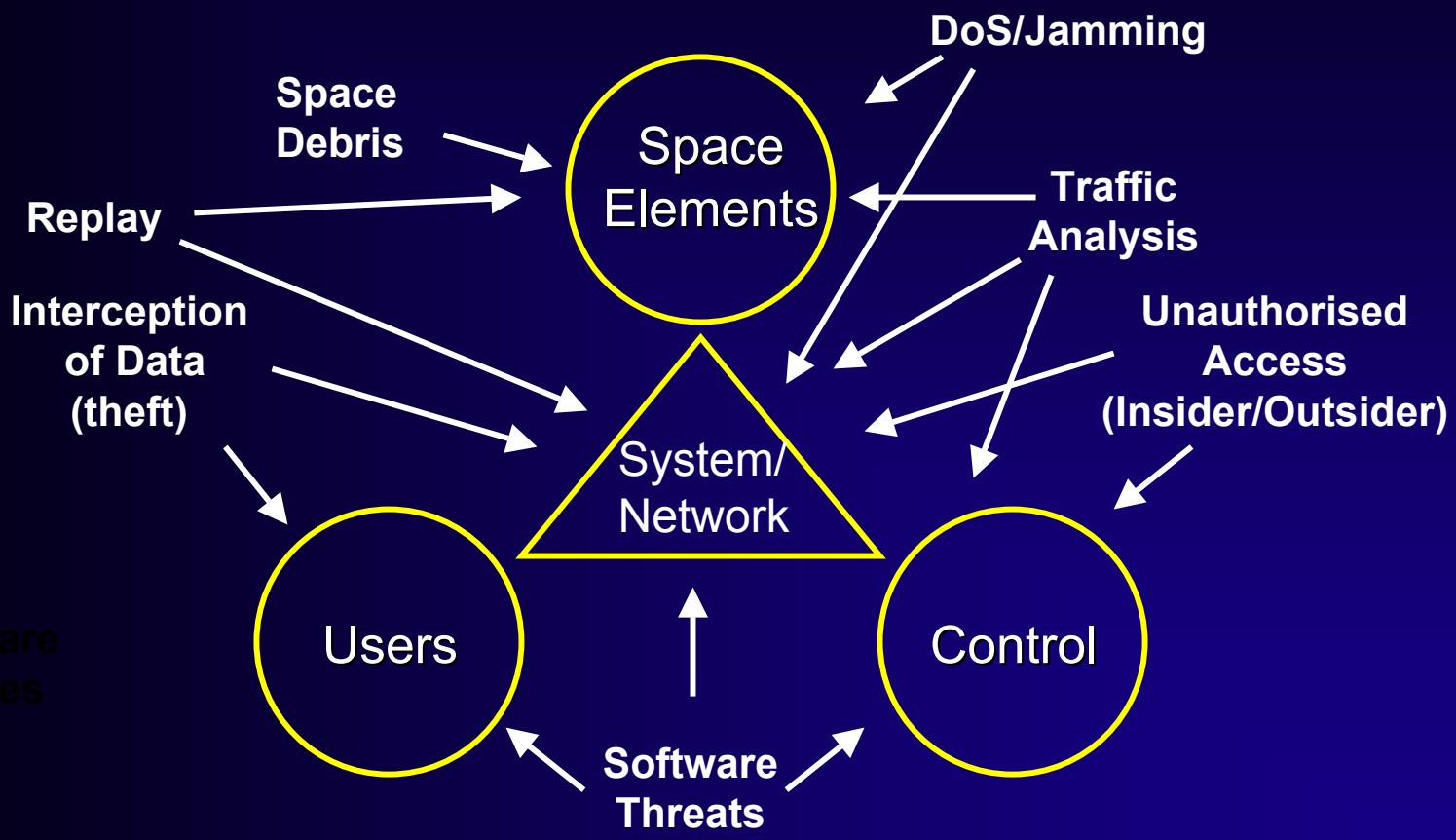
Background: Space Mission Security

- Civil mission security:
  - Almost non-existent in the past
    - "*our systems are so hard for us to manage that no one else will be able to figure them out*"
  - Acknowledgement that future missions require security – e.g., Space Station, weather satellites
- Military mission security:
  - Quite the opposite of civil missions
    - Security is a mandate

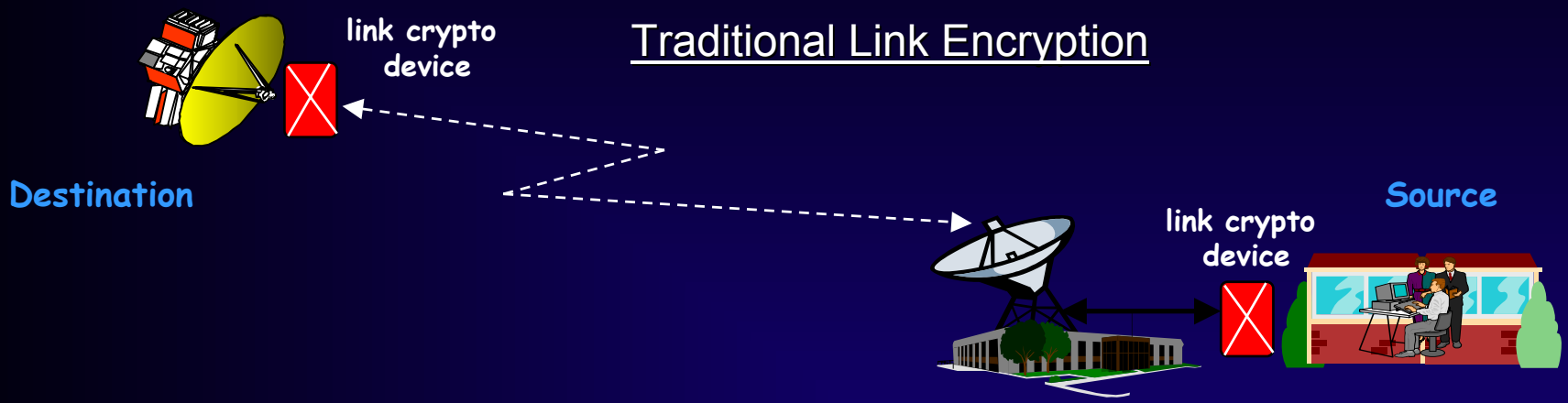
Space Security Issues

- Space missions need to protect
  - spacecraft and ground equipment
  - information and data contained within the systems
  - communications and data processing services
- Space mission security services are important
  - as network interconnectivity increases…
  - shouldn't wait for a problem to happen
  - must tailor to space mission application
- Security standardization is good
  - enables interoperability and compatibility
- Various layers possible for security services
  - application, network, data link/physical

Generic Threats to Space Missions

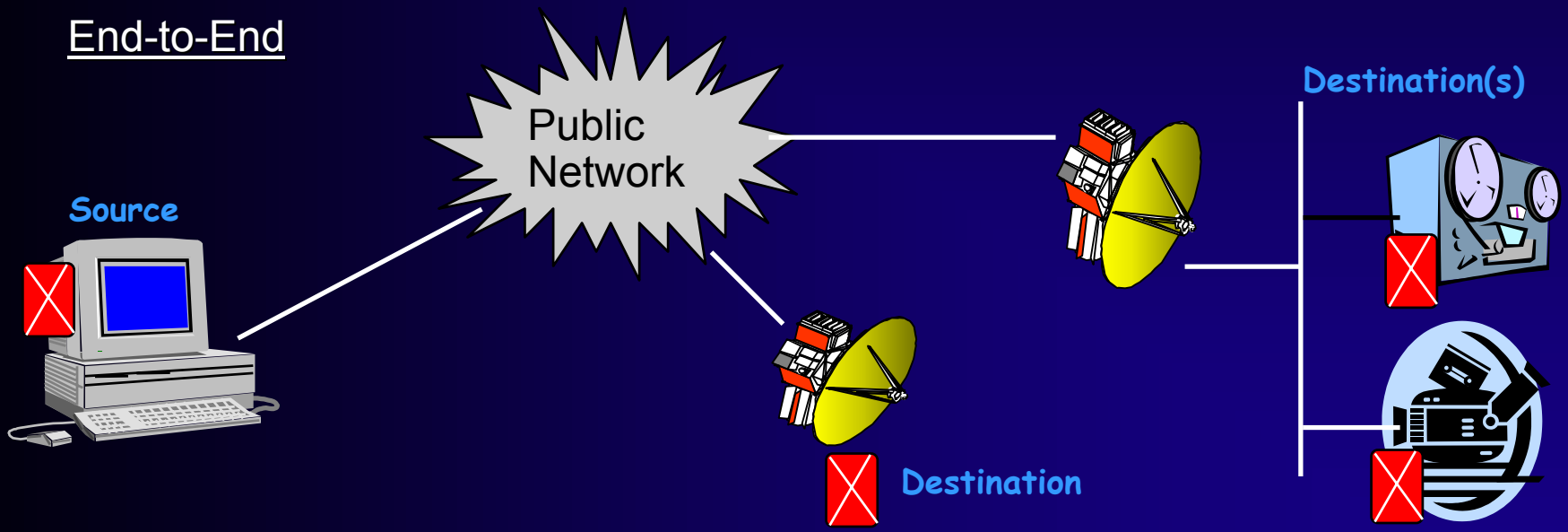


Security Paradigms



Security Paradigms (cont)

- End-to-End security
  - source to destination (writer to reader)
  - requires non-encrypted headers for routing (e.g., encryption above network or transport layer)



Applicable Security Standards

- IPSEC (Internet Protocol Security)
  - Internet standard security protocol
  - *Heavy* overhead - Assumes ground-based bandwidth availability
- SCPS-SP (DoD/NASA Space Communications Protocol Suite Security Protocol)
  - Light-weight IPSEC
  - CCSDS, ISO, and MIL standard
    - CCSDS 713.5-B-1
    - ISO 15892:2000
- CCSDS Layer 2 Packet Telemetry /Telecommand
  - Security layer above or below the transfer frame
  - ECSE (encrypted CCSDS Security Experiment)
- Military (NSA Type 1 equipments)
  - HAIPE – IPSec for military
- Application Layer: TLS/SSL

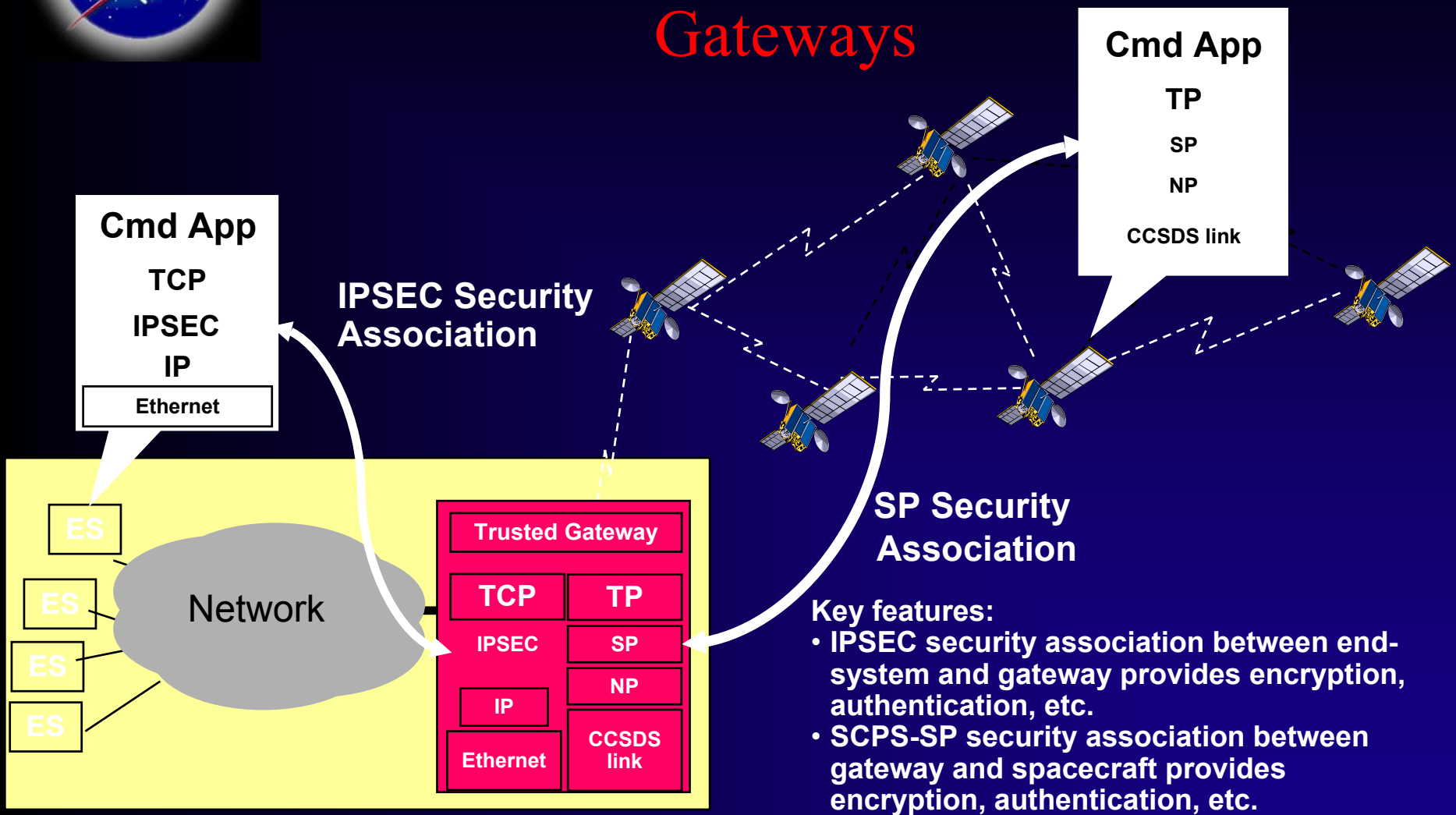
IPSEC Encapsulating Security Payload

- IETF (internet) ESP standard (RFC 2406)
  - Required in IPv6 (optional in IPv4)
- Designed for general Internet use
  - High bandwidth environments (e.g., fiber)
- Rich and robust (in terms of features)
- High protocol overhead
  - 10 bytes/packet (plus variable amount of padding and variable authentication data)

SCPS Security Protocol (SCPS-SP)

- ISO/CCSDS Standard
  - ISO 15892:2000
  - CCSDS 715.5-B-1
- Designed for space communications
  - Low bandwidth environments, short contact times
- Less rich and less robust than IPSEC ESP (in terms of features)
- Therefore, low protocol overhead
  - 2 bytes/packet (plus padding and authentication)

Gateways

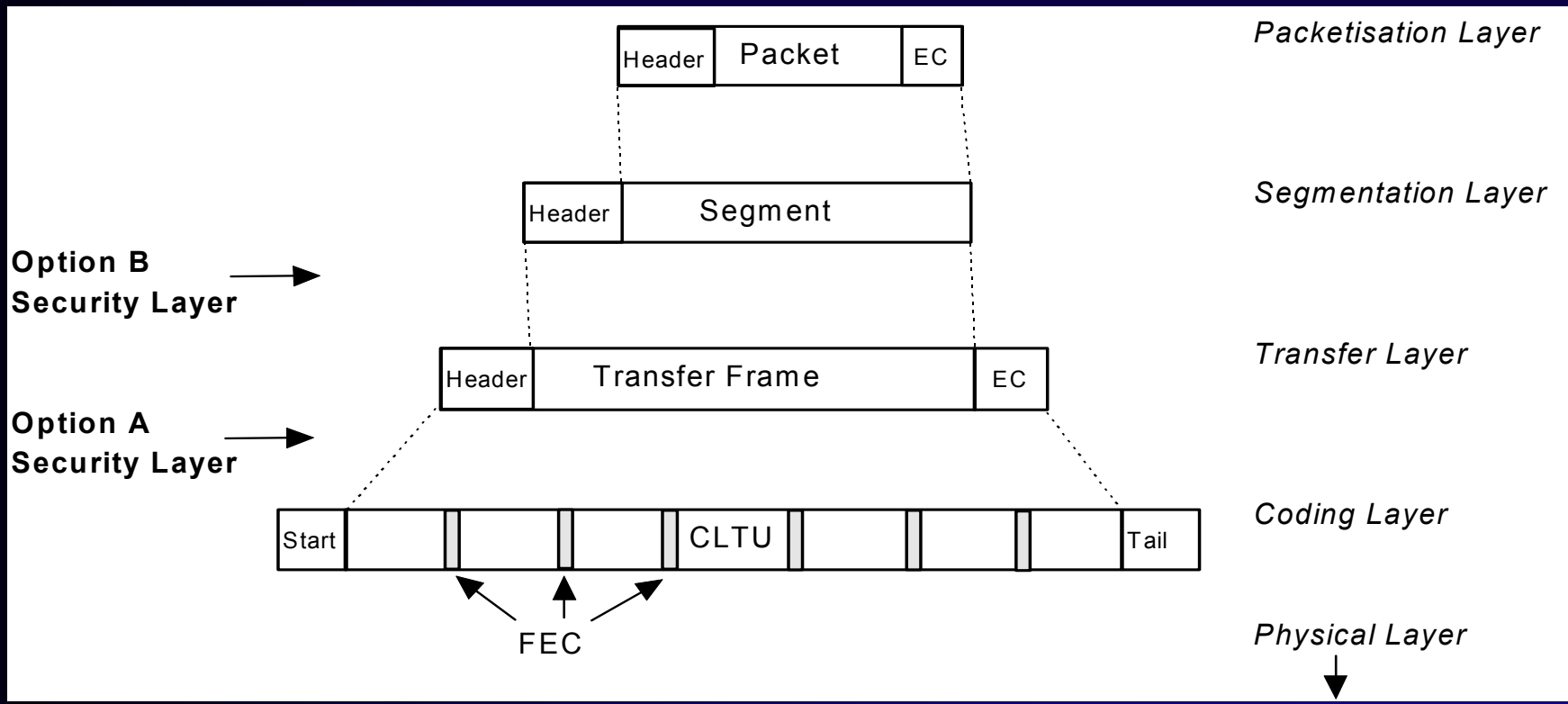


Key features:

- **IPSEC security association between end-system and gateway provides encryption, authentication, etc.**
- **SCPS-SP security association between gateway and spacecraft provides encryption, authentication, etc.**

CCSDS Layer 2 Security

- Conventional CCSDS telecommand and telemetry



Application Layer Security

- IETF Transport Layer Security (TLS)
  - RFC 2246
  - aka Secure Socket Layer (SSL)
  - "payload" encryption above the transport layer
    - Transport and below headers are untouched
  - Does not rely on any protocol stack mechanisms
  - Provides "writer to reader" security
  - But, each application has to re-invent the wheel (sort of)

Summary

- Security has been and is an integral part of Military space
  - Becoming more integral in Civilian space
- Standards-based options are available
  - Provides the ability to get out of the mode of reinvention for each mission.
  - Provides off-the-shelf solutions
  - Provides means of interoperability and cross-support

• NASA DATA SYSTEM STANDARDS PROGRAM •

1. Interplanetary Internet: An Architectural Framework for Space Internetworking: Adrian Hooke
2. User Data Services for Internet Based Spacecraft Applications: Joe Smith
3. CCSDS File Delivery Protocol (CFDP): Tim Ray
4. Internet Protocol Based Standards for Spacecraft Onboard Interfaces: Joe Smith
5. Standard Spacecraft Interfaces and IP Network Architectures: Jane Marquart
6. Standard Transport and Network Capabilities: Bob Durst
7. Next Generation Space Internet: Standards and Implementation: Keith Scott
8. Secure Space Networking: Howie Weiss
9. Delay Tolerant Networking: Scott Burleigh 
10. CCSDS Link Layer Protocol Suite: Greg Kazz